International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 10, Issue 2, March-April 2019, pp. 143-154. Article ID: IJARET_10_02_016
Available online at http://iaeme.com/Home/issue/IJARET?Volume=10&Issue=2
ISSN Print: 0976-6480 and ISSN Online: 0976-6499

A STUDY ON INTRUSION DETECTION

Dr Syeda Gauhar Fatima
Professor ECE dept, Deccan College of Engineering and Technology, Darussalam, Hyderabad, India

Syeda Kausar Fatima
Associate professor, Shadan College of Engineering and Technology, Hyderabad, India

Dr Syed Abdul Sattar
Principal, Nawab Shah Alam Khan College of Engineering and Technology, New Malakpet, Hyderabad, India

Syed Adil
Student, ECE dept, Deccan College of Engineering and Technology, Darussalam, Hyderabad, India.

ABTRACT

Intrusion Detection System (IDS) is meant to be a software application which monitors the network or system activities and finds if any malicious operations take place. Tremendous growth and practice of internet raises concerns about how to protect and communicate the digital data in a safe manner. Nowadays, hackers use different types of attacks for getting the valuable information. Many intrusion detection techniques, methods and algorithms assist to identify these attacks. This main objective of this paper is to provide a complete study about the description of intrusion detection, history, life cycle, types of intrusion detection methods, types of attacks, different tools and techniques, research needs, tasks and applications.

Keywords: Intrusion detection, IDS attacks, Functionality, Life cycle, Tools, Techniques.

Cite this Article: Dr Syeda Gauhar Fatima, Syeda Kausar Fatima, Dr Syed Abdul Sattar and Syed Adil, A Study on Intrusion Detection, *International Journal of Advanced Research in Engineering and Technology*, 10(2), 2019, pp. 143-154.
http://iaeme.com/Home/issue/IJARET?Volume=10&Issue=2

1. INTRODUCTION

An Intrusion Detection System is an application used for monitoring the network and shielding it from the intruder. With the quick progress in the internet based technology new application areas for computer network have emerged [7]. In some cases, the fields like business, financial, industry, security and healthcare sectors the LAN and WAN applications have advanced. All of these application areas made the network a striking target for the mishandling and a big

vulnerability for the community [7]. Malicious users or hackers use the organization's internal systems to collect information's and cause vulnerabilities like Software bugs, Delay in administration, leaving systems to default configuration [8]. As the internet developing into the society, new packages like viruses and worms are imported. The malignant so, the users use different procedures like cracking of password, identifying unencrypted text are used to cause vulnerabilities to the system. Hence, security is required for the users to secure their system from the intruders. Firewall technique is one of the widespread protection techniques and it is used to protect the private network from the public network. IDS are used in network related activities, medical applications, credit card frauds, Insurance agency [8].

The remaining portion of the paper is structured as follows. Section 2 tells about the history and the basic concepts of IDS. Section 3 explains the IDS functionality. Section 4 gives the brief description about the life cycle of IDS. Techniques are described in Section 5. Section 6 describes about IDS tools. Section 7 discusses the needs and challenges. Conclusion is given in Section 8.

2. HISTORY

The aim of intrusion detection is to monitor the network resources to detect anomalous behavior and misuse in network [16]. Intrusion detection theory was introduced in early 1980's after the evolution of internet with surveillance end monitoring the threat [17]. There was a abrupt rise in reputation and incorporation in security frame. Since then, several events in IDS technology have advanced intrusion detection to its current state [16]. James Anderson's wrote a paper for a government organization and introduced an approach that audit trails contained vital information that could be valuable in tracking misuse and understanding of user performance [16].

Then the detection appeared and audit data and its significance led to enormous improvements in the subsystems of every single operating system [16]. IDS and Host Based Intrusion Detection System (HIDS) were first defined. In 1983, SRI International and Dorothy Denning began working on a government project that launched a new effort into intrusion detection system development [17]. Around 1990s the revenues are generated and intrusion detection market has been elevated. Real secure is an intrusion detection network developed by ISS. After a year, Cisco recognized the priority for network intrusion detection and acquired the Wheel Group for achieving the security solutions [17]. The government actions like Federal Intrusion Detection Networks (FID Net) were designed under Presidential Decision Directive 63 is also adding impulse to the IDS [17].

3. INTRUSION DETECTION SYSTEM

An IDS is referred as burglar alarm. For example the lock system in the house safeguards the house from theft. But if somebody breaks the lock system and tries to enter into the house, it is the burglar alarm that detects that the lock has been broken and warns the owner by raising an alarm. Moreover, Firewalls do a very good job of filtering the incoming traffic from the Internet to circumvent the firewall [8]. For example, external users can connect to the Intranet by dialing through a modem installed in the private network of the organization; this kind of access cannot be identified by the firewall [8].

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that audits network traffic streams to detect and prevent vulnerability activities. There are two types of prevention system they are Network (NIPS) and Host (HIPS). These systems watch the network traffic and automatically take actions to protect networks and systems. IPS issue is false positives and negatives. False positive is defined to be an event which produces an alarm in IDS where there is no attack. False negative is defined to be an event which does not produces

an alarm when there is an attacks takes place. Inline operation can create blockages such as single point of failure, signature updates and encrypted traffic. The actions arising in a system or network is measured by IDS [8].

3.1. Types of IDS

Figure 1 shows the different types of Intrusion detection systems.

- Host based IDS
- Network based IDS
- Application based IDS

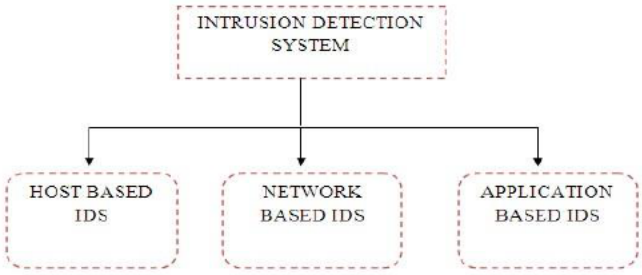

Figure 1 Intrusion Detection System – Types

Host based IDS views the sign of intrusion in the local system. For study they use host system's logging and other information. Host based handler is specified as sensor. Other sources, from which a host-based sensor can acquire data, include system logs and other logs generated by operating system processes and contents of objects not reflected in standard operating system audit and logging mechanisms [9]. Host based system trust strongly on audit trail. The information permits the intrusion detection system to spot subtle patterns of misuse that would not be noticeable at a higher level of abstraction [10]. The elementary principle in IDS including Network Based Intrusion Detection System (NIDS) initiated from anomaly HIDS research based on Denning's pioneering work [11]. A host-based IDS provides much more appropriate information than Network-based IDS. HIDS are used efficiently for examining the network attacks, for example, it can occasionally tell exactly what the attacker did, which commands he used, what files he accessed, rather than just an indefinite accusation and there is an attempt to execute a dangerous command [12]. It is less risky to configure.

3.1.1. Advantages of Host based Intrusion Detection Systems

- Verifies success or failure of an attack
- Monitors System Activities
- Detects attacks that a network based IDS fail to detect
- Near real time detection and response
- Does not require additional hardware
- Lower entry cost

Network based IDS systems gather information from the network itself relatively from each separate host [13]. The NIDS audits the network attacks while packets moving across the network. The network sensors come prepared with attack signatures that are instructions on what will constitute an attack and most network-based systems allow advanced users to define their own signatures [13]. Attack on the sensor is based on signature and they are from the previous attacks and the operation of the monitors will be translucent to the users and this is also significant [14].

The transparency of the monitors decreases the likelihood that an opponent will be able to locate it and invalidate its capabilities without the determinations [10]. Network Node IDS (NNIDS) agents are installed on every host within the network being protected [2].

3.1.2. Advantages of Network based Intrusion Detection Systems

- Lower Cost of Ownership
- Easier to deploy
- Detect network-based attacks
- Retaining evidence
- Real Time detection and quick response. Detection of failed attacks

Application based IDS (APIDS) will check the active behavior and event of the protocol [2]. The system or agent is placed between a process and group of servers that monitors and analyzes the application protocol between devices [2]. Intentional attacks are the malicious attacks carried out by disgruntled employees to cause harm to the system and Unintentional attacks causes financial damage to the system by deleting the important data file [2]. There are many attacks have taken place in OSI layer

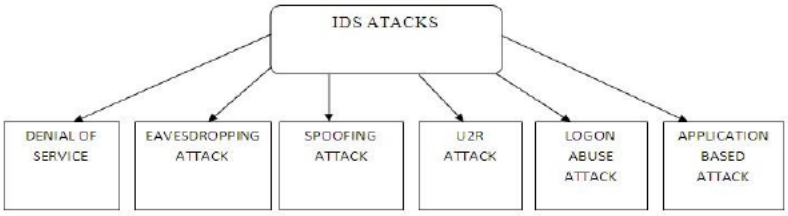

Figure 2 Intrusion Detection Attacks

3.2. Denial-of-Service (DOS) Attacks

It tries to deny the legal users from promoting the requested service. An advanced Distributed Denial of Service occurs in a distributed environment that the attacker sends or floods the server with many connections that request to knock the target system [2].Types of DOS attacks are

3.2.1. SYN Attack

SYN attack is also defined as Synchronization attack. Here, the attacker sends the flood of SYN request to the destination to use the resources of the server and to make the system unresponsive.

3.2.2. Ping of Death

In this the intruder sends a ping request to the targeted system which is larger than 65,536 bytes which causes the system to crash [2]. The formal size must be 56 bytes or 84 bytes in case of considering Internet protocol header.

3.3. Eavesdropping Attacks

It is the scheme of interference in communication by the attacker. This attack can be done over by telephone lines or through email. [2].

3.4. Spoofing Attacks

This attacker interprets as another user to forge the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a trusted user and provides access to the attacker [2].

3.5. Intrusion attacks or User to Root Attack (U2R)

An intruder tries to access the system or route through the network. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle which leads to loss of data [2].

3.6. Logon Abuse Attacks

A logon abuse attack would neglect the authentication and access control mechanisms and grant a user with more advantages [2].

3.7. Application-Level Attacks

The attacker targets the disabilities of application layer. For example, security weakness in the web server or in faulty controls on the server side [2].

4. FUNCTIONS OF IDS

The IDS consist of four key functions namely, data collection, feature selection, analysis and action, which is given in Figure 3.

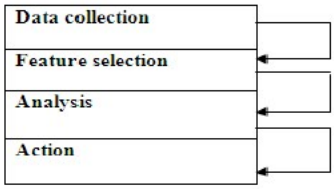

Figure 3 Functionality of IDS

4.1. Data collection

This module passes the data as input to the IDS. The data is recorded into a file and then it is examined. Network based IDS collects and modifies the data packets and in host based IDS collects details like usage of the disk and processes of the system**.**

4.2. Feature Selection

To select the specific feature large data is available in the network and they are frequently evaluated for intrusion. For example, the Internet Protocol (IP) address of the source and target system, protocol type, header length and size could be taken as a key for intrusion [15].

4.3. Analysis

The data is analyzed to find the accuracy. Rule based IDS examine the data where the incoming traffic is tested against predefined signature or pattern [15]. Another technique is anomaly based IDS where the system performance is studied and mathematical models are employed to it [15].

4.4. Action

It defines about the attack and reaction of the system. It can either inform the system administrator with all the obligatory data through email/alarm icons or it can play a dynamic part in the system by dropping packets so that it does not enter the system or close the ports [15].

5. IDS LIFE CYCLE

Vendors frequently release new IDS products aggressively and compete for market shares [19]. Estimating the new systems is not a relevant task and product calculation information is

imperfect. Hiring and retaining the workers to administer security and intrusion detection are the challenging tasks [19]. Faster changes in IT make it challenging for the firm to implement long term security strategy.

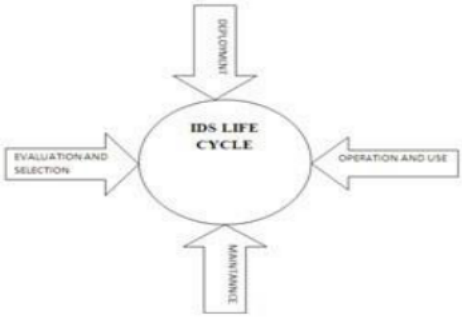

Figure 4 Functionality of IDS

5.1. Evaluation and Selection

If an organization plans to get IDS it should study the resources available for the systems operation and maintenance [19]. Lifecycle of a product for economic IDS is enhanced. The third-party evaluation is available and their reports are commonly on the surface [19]. This process illustrates about the finding of the intruder and the amount of work is necessary for maintaining the system in the network with traffic and the selection process defines about the identification of character, approaches, accuracy, usability, and effectiveness.

5.2. Deployment

Deployment phase includes the working of sensors to maximize protection for the serious assets by configuring the IDS to reflect security policy and installing signatures [19]. Users must develop rules for handling the alerts and to associate alerts with other systems. The Intrusion Detection Working Group of the Internet Engineering Task Force (IETF) is developing common alert format that uses the IDS to alert from different systems and they are reported to a common display console [19].

5.3. Operation and use

Organization administers the IDS to monitor the host and to respond the report as an alert. It establishes the roles and responsibilities for examining and monitoring the results of both manual and automatic responses [19]. Smart intruders who realize that IDS has been deployed on a network attack that they force it to provide false report [19].

5.4. Maintenance

Maintenance includes installation of signatures and IDS upgrades. Sensor placement should be revisited periodically to ensure that system or network changes [19]**.** An organization must attract, train and retain qualified technical staff to operate and maintain IDS technologies [19].

6. IDS TECHNIQUES

6.1. ANOMALY BASED INTRUSION DETECTION

Anomaly is indicated as an outlier, peculiarities or exceptions are the data pattern which performs abnormally. Anomaly detection technique is intended to uncover the patterns that are far from the normal and others are flagged as an intrusion [2]. Anomaly detections are classified into static and dynamic detectors.

Static anomaly detector is assumed as a portion of monitored system which remains constant. The static portion is possessed into two parts, i.e. system code and system data. Static portions of the system can be represented as a binary bit. If any divergence from its original form is occurred then the error has been indicated or the burglar has reshaped the portion of the system.

In dynamic detector the definition of the system behavior is included. The system behavior is defined as an order of different event. For example, audit records produced by the operating system are used by IDS to define the events of interest [2]. In this case, the behavior can be observed only when audit records are created by OS and the events are occurred in strict sequences [2]. If uncertain behavior is considered as anomalous, then the system administrators may be alerted by false alarms [3].

Anomaly detection is useful for finding attacks like misuse of protocol and service ports, DoS based on crafted payloads, DoS based on volume (DDoS), buffer overflow and other application payload anomaly.

6.2. Techniques used in anomaly detection

There are number of event and event counter are refined and have been implemented in anomaly detection.

6.2.1. Statistical Models

The statistical model shows the output as a statistical value. There are two types of statistical models, they are

6.2.1.1. Operational Model (or) Threshold Metric

The actions that occur over a period of time regulate the alarm. This can be visualized in Win2k lock; a user after n unsuccessful login attempts regulates the alarm. Here lower limit is 0 and upper limit is n [15].

6.2.1.2. Markov Process or Marker Model

In this model the system is inspected at fixed time intermission. The behavior is detected as anomaly if the probability of the state is low [15].

6.2.2. Cognition Models

6.2.2.1. Finite State Machine

A finite state machine (FSM) or finite automation is a model of behavior captured in states, transitions and actions [15]. A state defines about the past information. An action is a description of an activity that is to be performed at a given moment and the types of action are entry action, exit action and transition action [15].

6.2.2.2. Description Scripts

Scripting languages characterize the attacks on computers and networks. All scripting languages are capable of examining the sequences of specific events [15].

6.2.3. Cognition Based Detection Techniques

Cognition-Based (also called knowledge-based or expert systems) Detection Techniques work on the audit data [15]. The set of predefined rules for the classes and attributes are identified from training dataset [15].

6.2.3.1. Boosted Decision Tree or Boosted Tree (BT)

It uses ADA Boost (adaptive boosting) algorithm to generate many Decision Trees classifiers trained by different sample which is implemented in IDS [15].

6.2.3.2. Support Vector Machine (SVM)

SVM is defined to be the classifiers which are designed for the binary classification. Decision tree based SVM is a technique which merges the two techniques to solve the problem in an efficient way. The training and testing time can be decreased by using this method.

6.3. SIGNATURE BASED INTRUSION DETECTION

Signature based intrusion detection is termed as misuse detection. Here, the dataset has number of instances and every data must be labeled as normal or intrusive. The machine learning algorithms are used to train the data set according to their label. This technique automatically retains the signature to detect the intruder. Misuse detection technique is created automatically and the works are more complicated and precise than manually done [4]. Depending on the robustness and seriousness of a signature that is activated within the system, some alarm response or notification should be sent to the right authorities [4].

6.4. Techniques used in misuse detection

6.4.1. Expression matching

Expression matching is the easiest and simplest form in misuse detection. In this it searches for the stream of events like log entries for the happening of exact pattern.

6.4.2. State transition analysis

This model attacks the state or the transitions in the network. Every event in the network is applied to finite state machine instances which finally results in transition. An attack will be occurred when the machine reaches its final state.

6.5. TARGET MONITORING

Target monitoring is a technique which is used to report if any changes or modifications made in the system. This is usually done through cryptographic algorithm which computes a crypto checksum for each targeted file [5].If any changes are made in crypto checksum they are reported by IDS. Tripwire checksum is an integrity checker which checks for the changes or modification in the files.

6.6. STEALTH PROBES

A stealth probe is a technique used to collect and associates the data. It tries to find the attacks which has taken long period of time. Attackers will check for the system errors over a period of month, and wait for another two months to launch the attacks and they take a wide-area sampling and attempt to discover any correlating attacks [2].

7. TOOLS IN INTRUSION DETECTION

An intrusion detection product available today addresses a range of organizational security goals [2].This section discusses about the security tools.

7.1. SNORT

Snort is lightweight and open source software. Snort uses a flexible rule-based language to define the traffic [6].From an IP address; it records the packet in human readable form. Through

protocol analysis, content searching, and different pre-processors Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior [6].

7.2. OSSEC-HIDS

OSSEC (open source security) is free open source software. It will run on major operating system and uses a Client/Server based architecture. OSSEC has the ability to send OS logs to the server for analysis and storage. It is used in powerful log analysis engine, ISPs, universities and data centers. Authentication logs, firewalls are monitored and analyzed by HIDS.

7.3. FRAGROUTE

It is termed as fragmenting router. Here, from the attacker to the frag router the IP packet is sent and they are then fragmented and transformed to the party.

7.4. HONEYD

Honeyd is a tool that creates virtual hosts on the network [6]. The services are used by the host Honeyd allows a single host to request multiple addresses on a LAN for networks simulation. It is possible to knock the virtual machines or to trace route them [6]. Any type of service on the virtual machine can be simulated according to a simple configuration file [6].

7.5. KISMET

It is a guideline for WIDS (Wireless intrusion detection system).WIDS compromises with packet payload and happenings of WIDS. It will find the burglar access point.

8. NEEDS AND CHALLENGES

For employing an IPS device there are many challenges. The IPS device is designed to work inline presenting a potential choke point and single point of failure [18]. Some pursued attacks are undetected if the passive IDS fails and the network performances are impacted when the inline device fails. [18]. One of the components of network, the NIPS (Network intrusion prevention system) device must perform like a network switch. It must meet the network performance and consistency requirements to organize the challenges. Hence, very few customers are willing to sacrifice the network performance and consistency for security purposes [18].

A NIPS slows down the traffic and the issue of NIPS is dropped packets, they are used to complete data stream. Most high-end IPS vendors will get this problem by using custom hardware with advanced FPGAs and ASICs [18]. It is necessary to design the product to operate as an intrusion detection and prevention device [18]. Every organization needs IDS which is like a defense tool. There are some challenges the organizations face while deploying an intrusion detection system [8].

IDS technology itself is undergoing a lot of improvements. From the IDS operation it is understood that it is important for an organization. IDS technology does not need human interventions. Today an IDS technology offers some automation like notifying the administrator in case of detection of a malicious activity, shunning the malicious connection for a configurable period of time, dynamically changing a router's access control list in order to stop a malicious connection [8]. For every event occurrence the IDS logs should be monitored. Monitoring the logs on a daily basis is required to analyze the activities which are detected by the IDS over a period of time [8].

IDS operation depends on the deployment success. Planning plays a vital role for the design and operation phase. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS [8]. The decision can differ between organizations. A network based

IDS is an immediate choice for many organizations because of its ability to monitor multiple systems and also the fact that it does not require a software to be loaded on a production system unlike host based IDS [8].
Some of the organizations provide hybrid solution. So, the available resources are needed for a system before installing a host based sensor [8].

The ratio of sensor manager should be acclaimed. It is very important to design the standard policy before starting the IDS operation and avoid false positives result. IDS sensor may send a lot of false positives result to the sensor and the ratio can be insufficient [8].

The IDS technology is still reactive rather than proactive and this technology works on attack signatures [8]. Signatures are defined as a pattern of attacks which is defined earlier. The signature database needs to be updated whenever a different kind of attack is detected and they are fixed in the database and the frequency of signature update differs from vendor to vendor [8]. **5.** Because of collision domains in switched network the traffic in and out port cannot be seen from any other host port. But in HUB based network in and out can be viewed from any of the port. NIDS sensor needs to detect traffic in and out of a port and for the malicious traffic in the switched environment. For achieving this kind they use port mirroring or spanning [8].

9. IDS IN DIFFERENT DOMAINS

An IDS is used in many fields and the performance in each field is described and defines how they performed.

9.1. IDS in MANET

Manet is defined as mobile adhoc network. It is a self-directed network that is composed naturally by the combinations of mobile nodes without centralized administration. IDS is used in Manet. Mobile network is normally needed in the battleground for military people to get proper network [20]. Normally the messages are split into number of packet and they use a hardware device like wire and modem to transmit. But, in Manet they are connected wirelessly. Watchdog and path rater are the two techniques added on the protocol in Adhoc.

A watchdog detects the misbehaving nodes by eavesdropping on the transmission of the next hop [20]. A path rater then assist to find the routes that do not contain misbehaving nodes [20]. IDS are used in Manet while transferring the sequence of packets to the destination through mobile network to find the intruder if any.

9.2. IDS FOR CLOUD COMPUTING

Cloud computing is explained as internet based computing cloud where, virtual shared servers provide software infrastructure platform devices and other resources and hosting to customer as a service on pay-as you-use basis [21]. The user of the cloud does not hold any physical framework instead they lease from the mediator (third party). They pay only for the usage of the resource. Intrusion detection system plays an vital role in the security and perseverance of active defense system against intruder hostile attacks for any business and IT organization [24]. In cloud computing the applications are received on the remote server of the provider and they have the control headed for the usage of the data. IDMEF (Intrusion detection message exchange format) is the standard used in cloud for the communication purpose [21].

9.3. Cloud computing security issues

- Cloud data confidentiality
- Attacks on remote server
- Cloud security auditing

- Lack of data interoperability

9.4. IDS IN DATA MINING

Data mining is the process of extracting the concealed knowledge from the databases. IDS are very important in data mining. Intrusion detection includes identifying a set of malicious actions that compromise the integrity and availability of information resources [22].

Intrusion detection in data mining has two divisions, they are, misuse detection and anomaly detection. In misuse detection the labeled data are built using anticipating model [23]. In anomaly detection there is a deviation between models. To use the data first it should be converted into featured data and the data mining models are applied to it and they are summarized to produce the result.

9.5. TECHNICAL CHALLENGES

- Large data size
- Higher dimensionality
- Data preprocessing

10. CONCLUSION

The main objective of this paper is to provide an overview of the requirement and utility of intrusion detection system. This paper gives complete study about various types of IDS, life cycle, different domains, types of attacks and tools. IDS are becoming essential for day today security in corporate world and for network users**.** IPS defines about the preventing measures for the security. In the lifecycle the phases developed and the stages are illustrated. Still, there are more challenges to overcome. The techniques of anomaly detection and misuse detection are precisely illustrated and more techniques can be used. Further Work will be done on comparative analysis of some popular data mining algorithms applied to IDS and enhancing a classification based IDS using selective responses.

REFERENCES

[1] Corinne Lawrence- “IPS – The Future of Intrusion Detection”- University of Auckland - 26th October 2004.

[2] R, Karthikeyan & Indra, A. Intrusion Detection Tools and Techniques –A Survey. International Journal of Computer Theory and Engineering. 2. (2010). 901-906. 10.7763/IJCTE.2010.V2.260.

[3] Anita K. Jones and Robert S. Sielken –“Computer System Intrusion Detection A Survey” “International Journal of Computer Theory and Engineering, December, 2010 Vol.2, No.6,

[4] Vera Marinova-Boncheva-“A Short Survey of Intrusion Detection Systems”-. Bulgarian academy of sciences. (2007)

[5] Carl Endorf, Eugene Schultz, Jim Mellander “Intrusion detection & prevention” by Written-published by McGraw-Hill. (2006)

[6] “Top 125 Network Security Tools”- SecTools.Org- http://sectools.org/tag/ids/sec

[7] PeymanKabiri and Ali A.Ghorbani-“Research on Intrusion Detection and Response Survey”- International Journal of Network Security, Vol.1, No.2, Sep. 2005, Pp.84–102,

[8] Christopher Low –“Understanding Wireless attacks &detection”-GIAC Security Essentials Certification (GSEC) Practical Assignment 13 April 2005 -SANS Institute InfoSec Reading Room.

[9] Bace, Rebecca-“An Introduction to Intrusion Detection &Assessment”- Infidel, Inc. for ICSA, Inc. Pp, 1-38. (1999)

[10] Rebecca Gurley Bace-“Intrusion Detection”- Macmillan Technical Publishing, 2000.

[11] Denning, Dorothy E. – "An Intrusion Detection Model"- Proceedings of the Seventh IEEE Symposium on Security and Privacy May 1986
[12] "Global Information Assurance Certification Paper"- Copyright SANS Institute Copyright SANS Institute Author Retains Full Rights (2011)
[13] "SANS penetration testing copyright by SANS"-Copyright SANS Institute Author Retains Full Rights.
[14] Sriram Sundar Rajan, Vijaya Krishna Cherukuri-"An Overview of Intrusion Detection Systems".
[15] Asmaa Shaker Ashoor, Prof. Sharad Gore – "Importance of Intrusion Detection System"- International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.
[16] "Intrusion Detection and Intrusion Prevention"-Ed Sale VP of Security Pivot Group, LLC.
[17] John McHugh, Alan Christie, and Julia Allen- "The Role of Intrusion Detection Systems"- Software Engineering Institute, CERT Coordination Center.
[18] Shankar Sharan Tripathi, Sonu Agrawal- "A Survey on Enhanced Intrusion Detection System in Mobile Ad hoc Network"-International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 7, September 2012.
[19] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande – "Intrusion Detection System for Cloud Computing". International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012 ISSN 2277-8616 67 IJSTR©2012.
[20] Aleksandar Lazarević,Jaideep Srivastava, Vipin Kumar-"Data Mining for intrusion detection"Tutorial on the Pacific-Asia Conference on Knowledge Discovery in Databases 2003.
[21] Ms Asiya Jaleel -"Security Challenge in Cloud Computing"- Provided by International Journal of Engineering Sciences & Research Technology (IJESRT), Feb 2014
[22] Syeda Gauhar Fatima, Dr. Syed Abdul Sattar and Dr. K. Anita Sheela, Energy Efficient Intrusion Detection System For WSN, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 3, Issue 3, October-December (2012), pp. 246-250
[23] Jyoti Attri and Suman Kumari, Enhanced Power-Aware Hybrid Intrusion Detection Architecture in an Ad-Hoc Network Using Mobile Agents, International Journal of Computer Engineering and Technology (IJCET), Volume 5, Issue 7, July (2014), pp. 85-92
[24] Anurag, Hierarchical Intrusion Detection System in Cluster Based Wireless Sensor Network Using Multiple Mobile Base Stations, International Journal of Computer Engineering and Technology (IJCET), Volume 5, Issue 6, June (2014), pp. 82-87
[25] S. B. Patil, S. M. Deshmukh, Dr. Preeti Patil and Nitin Chavan, Intrusion Detection Probability Identification in Homogeneous System of Wireless Sensor Network, International Journal of Computer Engineering and Technology (IJCET), Volume 3, Issue 2, July- September (2012), pp. 12-18
[26] Taran Singh Bharati and R. Kumar. Intrusion Intrusion Detection System for Manet Using Machine Learning and State Transition Analysis. International Journal of Computer Engineering and Technology, 6(12), 2015, pp. 01-08.
[27] Ms. Trupti Phutane , Prof. Apashabi Pathan, Intrusion Detection System Using Decision Tree and Apriori Algorithm. International Journal of Computer Engineering and Technology, 6(7), 2015, pp. 09-18.
[28] Kushal Jani, Punit Lalwani, Deepak Upadhyay, Dr. M.B. Potdar, Performance Evolution of Machine Learning Algorithms for Network Intrusion Detection System. International Journal of Computer Engineering and Technology, 9(5), 2018, pp. 181-189
[29] Shraddha Chaurasia and Lalit Dole, Secure Masid: Secure Multi-Agent System for Intrusion Detection, International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 1, January- February (2013), pp. 392-397
[30] Jeena Kuriakose, Reshma Rajan and Gayathry K. V, Security in Manet Via Different Intrusion Detection Techniques, International Journal of Computer Engineering and Technology (IJCET), Volume 5, Issue 12, December (2014), pp. 82-87